IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellant:	Madhavan	Patent Application	
Serial No.:	10/656,041	Group Art Unit:	2419
Filed:	09/04/2003	Examiner:	Cho, Hong Sol

For: Automatic Provisioning of Network Address Translation Data

Appeal Brief

Table of Contents

Real Party in Interest

The assignee of the present invention is Hewlett-Packard Development Company, L.P., a Texas Limited Partnership.

Related Appeals and Interferences

There are no related appeals or interferences known to the Appellant.

Status of Claims

Claims 1-19 are pending. Claims 1-19 stand rejected. Rejections of Claims 1-19 are herein appealed.

Status of Amendments

All proposed amendments have been entered. An amendment subsequent to the Final Action has not been filed.

Summary of Claimed Subject Matter

Independent Claim 1 recites a method for automatically generating network address translation (NAT) data to enable a private host having a private IP address to communicate with a public host having a first public IP address, the private host being connected to a private network, the public host being connected to a public network. The method includes providing automated NAT provision software (402 of Figure 4 and paragraph 0022), the software, responsive to communication initiated by one of the private host and the public host, consulting (502 of Figure 5 and paragraph 0025) a security policy associated with the private host to determine whether the communication between the private host and the public host is permissible. The method further includes if the consulting (502 of Figure 5 and paragraph 0025) indicates that the communication between the private host and the public host is permissible, provisioning (506 of Figure 5 and paragraph 0026) automatically using the software and without a human operator intervention after the consulting, in a database a second public IP address for address translation between said private IP address and said second public IP address, said second public IP address being employed as one of a source IP address and a destination IP address for routing said communication between said private host and said public host through said public network.

Independent Claim 9 recites an article of manufacture comprising a program storage medium having computer readable code embodied therein, the computer readable code being configured to automatically generate network address translation (NAT) data to enable a private host having a private IP address to communicate with a public host having a first public IP address, the private host being connected to a private network, the public host being connected to a public network. The computer readable code for providing automated NAT provision software (402 of Figure 4 and paragraph 0022), the software consulting a security policy associated with the private host to determine whether communication between the private host and the public host is permissible and computer readable code for provisioning (506 of Figure 5 and paragraph 0026), in a database using the software, if the consulting indicates that the communication between the private host and the public host is permissible, a second public IP address for address translation between the private IP address and the second public IP address, the second public IP address being employed as one of a source IP address and a destination IP address for routing the communication between the private host and the public host through the public network.

Independent Claim 17 recites a method for automatically generating network address translation (NAT) data in a NAT table to enable communication between a private host having a private IP address and a public host having a first public IP address, the private host being connected to a private network, the public host being connected to a public network. The method includes consulting(502 of Figure 5 and paragraph 0025), using automated NAT provision software, a security policy associated with the private host to determine whether the communication between the private host and the public host is permissible, the consulting being performed responsive to a message initiated by one of the private host and the public host; and if the consulting indicates that the communication between the private host and the public host is permissible, provisioning (506 of Figure 5 and paragraph 0026) automatically using the software and without a human operator intervention after the consulting, in the NAT table a second public IP address for address translation between the private IP address and the second public IP address, the second public IP address being employed as one of a source IP address and a destination IP address for routing the communication between the private host and the public host through the public network.

Grounds of Rejection to be Reviewed on Appeal

1. Claims 1-7, 9-15 and 17-19 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Yanagidate (6,128,664) in view of Lee)7,047,561).

2. Claims 8 and 16 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Yanagidate (6,128,664) in view of Lee (7,047,561) and in further view of Aukia (7,047,561).

Arguments

1. Whether Claims 1-7, 9-15 and 17-19 are patentable over Yanagidate (6,128,664) in view of Lee)7,047,561).

"As reiterated by the Supreme Court in *KSR*, the framework for the objective analysis for determining obviousness under 35 U.S.C. 103 is stated in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966). Obviousness is a question of law based on underlying factual inquiries" including "[a]scertaining the differences between the claimed invention and the prior art" (MPEP 2141(II)). "In determining the differences between the prior art and the claims, the question under 35 U.S.C. 103 is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious" (emphasis in original; MPEP 2141.02(I)). Appellants note that "[t]he prior art reference (or references when combined) need not teach or suggest all the claim limitations, however, Office personnel must explain why the difference(s) between the prior art and the claimed invention would have been obvious to one of ordinary skill in the art" (emphasis added; MPEP 2141(III)).

Appellants respectfully submit that the claimed invention as a whole is not taught or suggested by Yanagidate and Lee. Independent Claims 1, 9 and 17 includes the feature of "consulting a security policy associated with the private host to determine whether a communication between the private host and the public host is permissible" and the Examiner indicates correctly that Yanagidate fails to teach or suggest this feature, as claimed. The Examiner indicates that Lee teaches this claimed feature.

While Lee may teach a firewall, Appellants respectfully submit that the differences between the combination of Yanagidate and Lee and the claimed invention would not be obvious to one of ordinary skill in the art. Specifically, the Examiner relies on Lee as teaching "consulting a security policy associated with the private host to determine whether a communication between the private host and the public host is permissible." Appellants respectfully disagree that Lee teaches this claimed feature.

In column 4, lines 37-47, Lee teaches "packet filter 106 examines address information contained in data packets.....to selectively control the flow of data." Additionally Lee states "packet filter 106 will follow predetermined security rules that specify which types of packets to allow to pass and which types to block\." With Lee, the packet data drives the filtering. This is very different from the claimed invention which "consults a policy associated with a host." Lee's filtering is packet based whereas the present claimed invention uses host policy to determine communication permissions.

Host policy based communication permissions is not taught or suggested by either Yanagidate or Lee. Thus, the invention, as a whole is not taught or suggested by Yanagidate in view of Lee.

For this rational, Appellants respectfully submit that Claims 1-7, 9-15, and 17-19 are patentable over Yanagidate in view of Lee and respectfully submit the rejection is improper and should be removed.

2. Whether Claims 8 and 16 are patentable over Yanagidate (6,128,664) in view of Lee (7,047,561) and in further view of Aukia (7,047,561).

As provided above, Appellants respectfully submit that neither Yanagidate nor Lee, alone and in combination teach or suggest the claimed feature of "consulting a security policy associated with the private host to determine whether a communication between the private host and the public host is permissible." Appellants respectfully submit that Aukia fails to remedy the deficiencies of Yanagidate and Lee in that Aukia fails to teach or suggest a host policy based communication permissions, as claimed.

For this rational, Appellants respectfully submit that Claims 8 and 16 are patentable over Yanagidate in view of Lee and yet in further view of Aukia and respectfully submit the rejection is improper and should be removed.

In summary, the Appellant respectfully requests that the Board reverse the Examiner's rejections of claims 1-19.

The Appellant wishes to encourage the Examiner or a member of the Board of Patent Appeals to telephone the Appellant's undersigned representative if it is felt that a telephone conference could expedite prosecution.

Respectfully submitted,

WAGNERBLECHER LLP

Date: 03/13/2009

/John P. Wagner, Jr./

John P. Wagner, Jr.

Registration Number: 35,398

WAGNERBLECHER
WESTRIDGE BUSINESS PARK
123 WESTRIDGE DRIVE
WATSONVILLE, CALIFORNIA 95076
408-377-0550

Claims Appendix

1. A method for automatically generating network address translation (NAT) data to enable a private host having a private IP address to communicate with a public host having a first public IP address, said private host being connected to a private network, said public host being connected to a public network, comprising:

providing automated NAT provision software, said software, responsive to communication initiated by one of said private host and said public host, consulting a security policy associated with said private host to determine whether said communication between said private host and said public host is permissible; and

if said consulting indicates that said communication between said private host and said public host is permissible, provisioning automatically using said software and without a human operator intervention after said consulting, in a database a second public IP address for address translation between said private IP address and said second public IP address, said second public IP address being employed as one of a source IP address and a destination IP address for routing said communication between said private host and said public host through said public network.

2. The method of claim 1 wherein said security policy is implemented using an access list.

3. The method of claim 2 wherein said second public IP address represents a shared public IP address if said communication is initiated by said private host.

4. The method of claim 2 wherein said second public IP address represents a dedicated public IP address if said communication is initiated by said public host.

5. The method of claim 1 wherein said database represents a Network Address Translation (NAT) table.

6. The method of claim 1 further including:

detecting a removal of said private host from said private network; and

removing, using said software, said second public IP address from said database responsive to said detecting said removal of said private host.

7. The method of claim 1 wherein said security policy represents a generic security policy.

8. The method of claim 7 further comprising automatically generating NAT data for all private hosts affected by said generic policy after said generic policy is modified using said software.

9. An article of manufacture comprising a program storage medium having computer readable code embodied therein, said computer readable code being configured to automatically generate network address translation (NAT) data to enable a private host having a private IP address to communicate with a public host having a first public IP address, said private host being connected to a private network, said public host being connected to a public network, comprising:

computer readable code for providing automated NAT provision software, said software consulting a security policy associated with said private host to determine whether communication between said private host and said public host is permissible; and

computer readable code for provisioning, in a database using said software, if said consulting indicates that said communication between said private host and said public host is permissible, a second public IP address for address translation between said private IP address and said second public IP address, said second public IP address being employed as one of a source IP address and a destination IP address for routing said communication between said private host and said public host through said public network.

10. The article of manufacture of claim 9 wherein said security policy is implemented using an access list.

11. The article of manufacture of claim 10 wherein said second public IP address represents a shared public IP address if said communication is initiated by said private host.

12. The article of manufacture of claim 10 wherein said second public IP address represents a dedicated public IP address if said communication is initiated by said public host.

13. The article of manufacture of claim 9 wherein said database represents a Network Address Translation (NAT) table.

14. The article of manufacture of claim 9 further including:

computer readable code for detecting a removal of said private host from said private network; and

computer readable code for removing, using said software, said second public IP address from said database responsive to said detecting said removal of said private host.

15. The article of manufacture of claim 9 wherein said security policy represents a generic security policy.

16. The article of manufacture of claim 15 further comprising computer readable code for automatically generating NAT data for all private hosts affected by said generic policy after said generic policy is modified using said software.

17. A method for automatically generating network address translation (NAT) data in a NAT table to enable communication between a private host having a private IP address and a public host having a first public IP address, said private host being connected to a private network, said public host being connected to a public network, comprising:

consulting, using automated NAT provision software, a security policy associated with said private host to determine whether said communication between said private host and said public host is permissible, said consulting being performed responsive to a message initiated by one of said private host and said public host; and

if said consulting indicates that said communication between said private host and said public host is permissible, provisioning automatically using said software and without a human operator intervention after said consulting, in said NAT table a second public IP address for address translation between said private IP address and said second public IP address, said second public IP address being employed as one of a source IP address and a destination IP address for routing said communication between said private host and said public host through said public network.

18. The method of claim 17 wherein said second public IP address represents a shared public IP address if said communication is initiated by said private host.

19. The method of claim 17 wherein said second public IP address represents a dedicated public IP address if said communication is initiated by said public host.

Evidence Appendix

None

Related Proceedings Appendix

None